



D-1181 R1

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

In re Application of:)
 Ramachandran, et al.)
)
Application No.: **10/601,813**) Art Unit 2876
)
Confirmation No.: **9839**)
)
Filed: **June 23, 2003**) Patent Examiner
) Daniel Hess
)
Title: **Automated Banking Machine**)
 With Improved Resistance)
 To Fraud)

Mail Stop Appeal Brief - Patents
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

**SUPPLEMENTAL BRIEF OF APPELLANTS
PURSUANT TO 37 C.F.R. § 41.37**

Sir:

The Appellants hereby request reinstatement of their appeal. The Appellants hereby submit their Supplemental Appeal Brief pursuant to 37 C.F.R. § 41.37 concerning the above-referenced Application. This Supplemental Appeal Brief is in response to the Office Action dated May 3, 2006.

(i)

REAL PARTY IN INTEREST

The Assignee of all right, title and interest to the above-referenced Application is Diebold, Incorporated, an Ohio corporation.

(ii)

RELATED APPEALS AND INTERFERENCES

Appellants, Appellants' legal representative, and assignee believe that there are no related appeals or interferences pertaining to this matter.

(iii)

STATUS OF CLAIMS

Claims 1-38 are pending in the Application.

Claims rejected: 1-37

Claims allowed: none

Claims confirmed: none

Claims withdrawn: 38 (Rejoinder thereof is respectfully requested)

Claim objected to: none

Claims canceled: none

Appellants appeal the rejections of claims 1-37, inclusive. These rejections were the only rejections present in the Office Action (“Action”) dated May 3, 2006, which reopened prosecution yet was made Final.

(iv)

STATUS OF AMENDMENTS

The Action dated May 3, 2006 included a final rejection. No claim amendments were requested to be admitted after the final rejection.

(v)

SUMMARY OF CLAIMED SUBJECT MATTER

Concise explanations of exemplary forms of the claimed invention:

For reasons of brevity, claim language may be referred to herein (and in Appellants' arguments) in a shortened version. For example, language such as "at least one" may be simply referred to as "a". Any generalized statement in this Appeal Brief is not to limit any of the mentioned claims in any manner. Please refer to the specific claim for the exact claim language.

With respect to independent claim 1

An exemplary form of the invention is directed to an automated banking machine apparatus. The automated banking machine apparatus (e.g., 10; Figure 1) comprises a user interface (24) in supporting connection with a housing (12). The user interface (24) includes an input device and an output device (e.g., display 36). The input device includes a card reader (26; Figure 3). The card reader (26) has an associated card reader slot (28; Figures 1, 14, 15) that is adapted to accept user cards. A radiation emitting device (126; Figures 14-15) is positioned adjacent the slot (28). A radiation sensing device (128; Figures 14-15) is also adjacent the slot (28) such that positioning an unauthorized card reading device (130; Figure 15) adjacent the slot (28) causes a change in a property of radiation (that was emitted) from the radiation emitting device (126) to be sensed by the radiation sensing device (128) (e.g., Specification page 27, lines 7-15). A controller (72; Figure 3) is in the housing (12). The controller (72) is in operative connection with the radiation sensing device (128) (e.g., page 26, lines 9-10). The controller (72) is operative to generate a signal responsive to a sensed property change to indicate installation of an unauthorized card reading device (130) adjacent the card reader slot (28) (e.g., page 29, line 3 to page 30, line 14). Particularly note page 25, line 5 to page 30, line 14.

With respect to independent claim 16

Another exemplary form of the invention is directed to an automated banking machine apparatus. Support in the disclosure for like reference numerals have previously been provided. The apparatus includes a housing (12), user interface (24), card reader (26), card reader slot (28), output device (e.g., display 36), radiation emitting device (126), sensing device (e.g., 128), and controller (72).

The controller (72) is operative to cause prompting of a user to move a card in the slot (e.g., page 26, lines 2-4) and selectively cause operation of the radiation emitting device (e.g., page 26, lines 1-2; page 28, lines 1-4), where the operation is dependent on the prompting. The controller is operative to cause an output responsive to a sensing of an unauthorized card reading device (130) (e.g., page 29, line 3 to page 30, line 14).

With respect to independent claim 19

Another exemplary form of the invention is directed to an automated banking machine apparatus. Support in the disclosure for like reference numerals have previously been provided. The apparatus includes a slot member (e.g., 66) on a user interface (24) and bounding at least one side of a slot (28). A sensor device is positioned to detect an unauthorized object (130) placed adjacent the user interface (24). The sensor device includes a radiation emitting device (126) and a radiation sensing device (128) mounted in supporting connection with the slot member (e.g., 66) (Figures 1 and 14-15). The controller (72) is operative to selectively control the sensor device.

With respect to independent claim 23

Another exemplary form of the invention is directed to an automated banking machine apparatus. Support in the disclosure for like reference numerals have previously been provided. The apparatus includes a housing (12), user interface (24), card reader (26), card reader slot (28), and an output device (e.g., display 36). A sensing device (e.g., 128) positioned adjacent the card reader slot (28) is adapted to sense an unauthorized card reading device (130). A controller (72) is in the housing (12) and in operative connection with the sensing device (128). The controller (72) is operative to execute fuzzy logic (e.g., page 26, lines 15-17; page 28, lines 5-7) in comparing a stored value with a current value that corresponds to a signal currently produced by the sensing device (128). The controller (72) is further operative to produce an output responsive to a result of the comparison (e.g., page 29, line 3 to page 30, line 14).

With respect to independent claim 26

A further exemplary form of the invention is directed to a method. Support in the disclosure for like reference numerals have previously been provided. The method includes sensing with a sensing device (e.g., 128) adjacent to a card reader slot (28) of a user interface (24) of an automated banking machine (e.g., 10), an unauthorized card reader device (130) attached to the user interface. The sensing includes emitting radiation with an emitting device (126) located adjacent the slot (28). The sensing also includes sensing radiation from the emitting device (126) with a radiation sensor device (128) located adjacent the slot (28) and the emitting device (126). The sensing device is selectively controlled by a controller (72) of the

machine. The method further includes, responsive to sensing the unauthorized card reader device (130), providing at least one output from the machine (e.g., page 29, line 3 to page 30, line 14).

With respect to independent claim 32

A further exemplary form of the invention is directed to a method. Support in the disclosure for like reference numerals have previously been provided. The method includes operating a sensing device (e.g., 128) adjacent to a card reader slot (28) of a user interface (24) of an automated banking machine (e.g., 10). The method also includes executing fuzzy logic in comparing at least one property (sensed with the sensing device) to a stored value in determining whether an unauthorized card reader device (130) is attached to the user interface (24). The method further includes, responsive to determining that an unauthorized card reader device (130) is attached, providing an output from the machine (e.g., page 29, line 3 to page 30, line 14).

With respect to independent claim 35

A further exemplary form of the invention is directed to a method. Support in the disclosure for like reference numerals have previously been provided. The method includes operating a sensing device (e.g., 128) adjacent to a card reader slot (28) of a user interface (24) of an automated banking machine (e.g., 10) in a transaction step in which a card is to be moved in the card reader slot (28). The method also includes determining that an unauthorized card reader device (130) is attached to the user interface (24) responsive to the operating step. The method further includes, responsive to the determining step, capturing a card (that has been subject to

being read by the unauthorized reading device 130) through operation of the machine (e.g., page 30, lines 18-21).

With respect to independent claim 36

A further exemplary form of the invention is directed to a method. Note claim 35 for support for steps (a) and (b). Step (c) includes, responsive to the determining step, cancelling an account associated with a card that has been subject to being read by the unauthorized reading device (130) (e.g., page 30, lines 1-21).

With respect to independent claim 37

A further exemplary form of the invention is directed to a method. Note claim 35 for support for steps (a) and (b). Step (c) includes, responsive to the determining step, monitoring activity on an account associated with a card that has been subject to being read by the unauthorized reading device (130) (e.g., page 30, lines 6-8).

(vi) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The questions presented in this appeal are:

- 1). Whether claims 1-2, 14-19, 24, 26, 29, and 32 are unpatentable pursuant to 35 U.S.C. § 102(e) as being anticipated by Mair, et al. (US 6,367,695) (hereinafter "Mair").
- 2). Whether claims 3-13, 20-23, 25, 27-28, 30-31, and 33-37 are unpatentable pursuant to 35 U.S.C. § 103(a) as being obvious in view of Mair.

(vii)

ARGUMENT

The 35 U.S.C. § 102(e) Rejections

The Applicable Legal Standards for 35 U.S.C. § 102 Rejections

Anticipation pursuant to 35 U.S.C. § 102 requires that a single prior art reference contain all the elements of the claimed invention arranged in the manner recited in the claim. *Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 1548, 220 USPQ 193, 198 (Fed. Cir. 1983).

Anticipation under 35 U.S.C. § 102 requires in a single prior art disclosure, each and every element of the claimed invention arranged in a manner such that the reference would literally infringe the claims at issue if made later in time. *Lewmar Marine, Inc. v. Barient, Inc.*, 827 F.2d 744, 747, 3 USPQ2d 1766, 1768 (Fed. Cir. 1987).

Anticipation by inherency requires that the Office establish that persons skilled in the art would recognize that the missing element is necessarily present in the reference. To establish inherency the Office must prove through citation to prior art that the feature alleged to be inherent is "necessarily present" in a cited reference. Inherency may not be established based on probabilities or possibilities. It is improper to reject a claim on the basis of § 102 based merely on the possibility that a particular prior art disclosure could or might be used or operated in the manner recited in the claim. *In re Robertson*, 169 F.3d 743, 49 USPQ2d 1949 (Fed. Cir. 1999).

It is respectfully submitted that the Action from which this appeal is taken does not meet these burdens.

Mair does not anticipate the claims

Appellants' remarks in their 1st Appeal Brief filed March 3, 2006 are incorporated herein by reference.

Claim 1

The Action (e.g., at pages 3 and 12) makes clear that Mair's Figure 3 embodiment is the only portion of Mair that is relied upon in the rejection . Appellants agree with the Office that Mair's Figure 2 embodiment is non analogous to the recited invention of claim 1.

Mair does not teach having *both* a radiation emitting device and a radiation sensing device positioned adjacent a card reader slot

Mair does not teach a radiation emitting device and a radiation sensing device, where *both* devices are positioned adjacent the same card reader slot (e.g., Appellants' Figure 14). Claim 1 specifically recites a "radiation emitting device positioned *adjacent* the slot". However, in Mair's Figure 3 the emitter (108) is specifically positioned operationally *away* from the card reader slot (12) for concealment behind the distant monitor screen (116) (e.g., col. 5, lines 29-31). One having ordinary skill in the art would understand that Mair's emitter (108) is not positioned *adjacent* the card reader slot (12). Thus, Mair does not teach the recited features. Nor can Mair anticipate claim 1.

Furthermore, Mair structurally teaches against the recited invention. For example, note Mair's operational alignment of the detector (102) and the emitter (108) in Figure 3 (and the similar alignment in Figure 2). One having ordinary skill in the art would recognize that the size of Mair's detector (102) and emitter (108) would prevent their operational positioning adjacent to

the card reader slot (12), which is located at the open face of the ATM fascia. For example, how could the emitter (108) be supported adjacent the slot (12)? Where is there any support structure (that could support the emitter 108) located adjacent the side of the slot (12) opposite the detector (102)? There is isn't any. The side of the slot (12) opposite the detector (102) is open to the environment, else a user could not insert their card into the slot (12). As a result, not only does Mair lack the recited apparatus, but Mair also teaches away from any capability of being structurally modified to produce the recited apparatus.

Mair does not teach signal generation responsive to sensing radiation

Claim 1 recites that a radiation sensing device is adjacent the card reader slot such that a positioning of an unauthorized card reading device adjacent the slot causes a change in at least one property of radiation (that was emitted from the radiation emitting device) that is sensed by the radiation sensing device. Claim 1 further recites that a controller is operative to generate a signal responsive to the sensed change, whereby installation of an unauthorized card reading device adjacent the card reader slot is indicated.

That is, in the recited arrangement an unauthorized card reading device positioned adjacent the card reader slot causes: a change in a property of emitted radiation; a sensing of the change by a radiation sensing device; and a generation of a signal (indicative of the unauthorized card reading device) responsive to the sensed change. Conversely, in Mair's arrangement a false sheet (118) causes: an interruption of emitted signals so they don't reach the detector (102) (col. 5, lines 41-42); an absence of sensing radiation with the detector (102); and a remotely located alarm generation responsive to the absence of sensed radiation.

In claim 1 an unauthorized card reading device is detected because of a sensing of radiation by a radiation sensing device. Detection is based on the "radiation sensing" device having "sensed". Conversely, in Mair's arrangement (col. 5, lines 15-44) a false sheet (118) is detected because of a lack of sensing of signals by a detector (102). Mair's arrangement is based on emitted signals not reaching the detector (col. 5, lines 1 and 39-44). That is, alarm generation in Mair is based on emitted signals not being sensed.

Again, in claim 1 the signal generation is based on emitted radiation being "sensed" by the radiation sensing device. If Mair's emitted signals don't reach the detector, then how can these signals be "sensed" by the detector to cause alarm generation? They can't. Nor can Mair teach the recited features and relationships in claim 1. It follows that Mair cannot anticipate claim 1.

Mair does not teach sensing "a change in at least one property of radiation"

In claim 1 the radiation sensing device senses a "change in at least one property of radiation". Further, the indicative signal is generated responsive to this sensed change. Where does Mair's detector (40) sense a "change in at least one property of radiation"? As previously discussed, Mair's alarm generation is based on not sensing *any* radiation with a detector, let alone sensing a "change in at least one property of radiation". If Mair doesn't sense radiation with a detector, then how can he sense a "change in at least one property of radiation" with the detector? He can't. Where does Mair sense radiation that has been changed, especially with a "radiation sensing" device? He doesn't. In Mair there is no sensing of a changed property of radiation by a "radiation sensing" device. Furthermore, if Mair doesn't sense radiation with the detector (40),

then how can the detector (40) constitute a "radiation sensing" device? Mair does not teach the recited features and relationships. It follows that Mair cannot anticipate claim 1.

Mair is not directed to detecting an unauthorized card reading device

Mair is directed to preventing unauthorized capture of both a magnetic strip card and the PIN associated with the card (col. 1, lines 19-27 and 36-40; col. 4, lines 4-7). Mair teaches (at col. 4, lines 4-7) that a false capture device can be a "data capture device" or a "token capture device for *capturing . . . a magnetic stripe card*".

Mair indicates that a false keypad (21) can be fraudulently used to capture a card's PIN data. It follows that the embodiment of Figure 2 is directed to a "data capture device" being the false keypad (21), which captures PIN data.

Mair further indicates that a false sheet (118) having a false card reader slot can be fraudulently used to physically capture an entire card. It follows that the embodiment of Figure 3 is directed to a "token capture device" being the false sheet (118), which captures (and keeps) a "magnetic stripe card". The false sheet (118) is a card stealing device.

Mair desires to prevent unauthorized capture a card and its PIN data (col. 1, lines 36-40). As a result, Mair tries to prevent use of both a false keypad (21) (which is used to capture a card's PIN data) and a false cover sheet (118) (which is used to capture the physical card).

Mair is not concerned with unauthorized reading of a card with a false card reading device. Where does Mair teach use of an unauthorized *card reading* device? There is no teaching in Mair of preventing fraudulent *reading* of a card at the ATM. At best, Mair is

concerned with preventing the physical *capture* of a card by a false sheet (118) having a false card entry slot (Figure 3).

Even Mair acknowledges the "false card reader slot" (col. 5, line 40). Mair is concerned with a false card entry "slot" in a card stealing device (118), not a false card "reader". There is no teaching in Mair that an unauthorized card reading device is part of the false card slot or the false sheet (118). Mair's false card slot (118) is just that, a false slot through which a card can be inserted so that it can be physically captured (not read) by the false sheet (118). Mair's false sheet (118) has a slot through which an ATM user inserts (and loses) their card. The false sheet (118) doesn't read anything, especially a card.

Mair's concern about preventing the capture of the entire card further indicates that he is not concerned about preventing a reading of the card. Why would Mair prevent card reading but allow theft of the card, especially when the stolen card can be read later? Again, the card stealing device (118) is limited to physically keeping a card. There is no need for the card stealing device (118) to read a card.

Mair is non analogous to the problem and environment of unauthorized card reading devices. It follows that Mair cannot teach an ability to sense an unauthorized card reading device. Mair cannot anticipate claim 1.

Mair structurally teaches against the recited invention

Mair's structure teaches away from the false sheet (118) being a false card reader. Mair's false sheet (118) is sized to capture (and hide) an entire card therein. To carry out such theft, the card stealing device (118) has to be large (i.e., larger than a card). As shown in Mair's Figure 3,

the large size needed for the card stealing device (118) appears to require that it extend across the entire ATM fascia. Even Mair acknowledges that the false sheet (118) "is placed over the [entire] lower part of the ATM" (col. 5, lines 39-41). The Office has presented no evidence that a false card *reader* would need to cover such a large area, especially a false card reader that only needs to cover the (much smaller) card entry slot.

As can be seen, the size of Mair's card stealing device (118) (Figure 3) is much larger than the smaller keypad (16) and the card reader slot (12) (Figure 1). Mair's Figure 1 also shows that the card reader slot (12) is even smaller in area than the keypad (16). Thus, it would appear that a false card *reader* (which Mair does not teach) could be even smaller than Mair's false keypad (21). The Office has presented no evidence whatsoever that Mair's Figure 3 detection arrangement could detect such a small false card reader.

Furthermore, it appears that in Mair's Figure 3 the emitter (108) and the detector (102) are out of alignment with the card reader slot (12) entry. How in Mair could a false card reader (that only extends across or covers the card reader slot entry) be detected if the emitter/detector alignment doesn't even pass through the slot entry? Mair does not anticipate claim 1.

Mair does not teach the recited controller

For reasons discussed above, Mair does not teach the radiation emitting device and radiation sensing device positional relationship. Nor does Mair teach sensing a change in a property of radiation". It follows that Mair cannot teach a controller that is in operative connection with the radiation sensing device and can generate a signal responsive to the change.

It further follows that Mair cannot indicate installation of an unauthorized card reading device adjacent a card reader slot. Mair cannot anticipate claim 1.

The Action (on page 4) alleges that Mair has a controller (112) that generates an alarm signal "which clearly is indicative of an unauthorized card reading device: Mair et al. uses the term 'false card reader slot' which is the same thing". The Appellants respectfully disagree.

For reasons previously discussed, Mair does not teach that the alarm signal indicates an unauthorized card *reading* device. At best, the alarm merely indicates possible detection of a card stealing device (118) that requires a size so large (in order to hide a card) that it covers the entire lower area of the ATM (col. 5, lines 39-41).

Nor is the term "false card reader slot" the same thing as an "unauthorized card reading device", as alleged by the Office.

One having ordinary skill in the art would understand that there are different types of fraud devices associated with ATMs. For example, there is: (1) a device for stealing non-card data (like Mair's false keypad 21, which records a manually entered PIN); (2) a device for stealing an entire card (like Mair's false sheet 118, which physically retains a captured card); and (3) a device for stealing card data (like the unauthorized card reading device 130 shown in Appellants' Figure 15, which reads data from a card, without stealing the card). The Office appears to have confusion distinguishing between these different devices (1), (2), and (3). At best Mair relates to described devices (1) and (2), but not to device (3). Claim 1 relates to device (3). Again, Mair does not anticipate claim 1.

Mair's arrangement cannot address the problem solved by Appellants' invention

One having ordinary skill in the art would recognize that Mair's detection arrangement can be easily evaded, rendering it useless for its intended purpose. For example, Mair's detection approach can be easily evaded by placing a fiber optic strand through the large area between the emitter and the detector. Mair's allocated delay period (col. 5, lines 4-10 and 46-53), in which an alarm is prevented, provides ample time for such a strand installment. In contrast, in an exemplary arrangement of Appellants' invention *both* the emitting device and the sensing device are adjacent the card reader slot. Thus, the exemplary arrangement renders a fiber optic strand useless because it would interfere with (and prevent) card entry into the slot. It follows that Appellants' exemplary form of the invention further distinguishes from Mair.

Claim 1 conclusion

Mair cannot anticipate claim 1. The Office's need to rely on obviousness (e.g., in the Office Action dated October 6, 2005) when previously applying Mair alone is further evidence against the allegation of anticipation. Appellants respectfully submit that in light of the failure of the solely applied reference to teach all of the recited features and relationships, combined with the lack of any other evidential support of record for the rejection, the anticipation rejection is not legally valid. Thus, Appellants respectfully submit that the claim 1 rejection should be reversed.

Claim 2

Since Mair does not teach the recited apparatus of claim 1, Mair further cannot teach the additional currency dispensing device of claim 2, which depends on claim 1. The Office has not established a *prima facie* case of obviousness.

Claim 14

Mair further does not teach a radiation emitting device and a radiation sensing device mounted in supporting connection with a housing member that *bounds* at least one side of a card reader slot. The Action is silent as to what constitutes the recited housing member. Nor is Mair's emitter (108) and detector (102) mounted in supporting connection with a housing member that bounds a card reader slot. Mair does not anticipate claim 14.

Claim 15

Claim 15 depends from claim 14/1. Mair further does not teach a housing member extending in *surrounding* relation of a card reader slot. The Action's reference to Figure 1 is deficient. Figure 1 does not show a housing member bounding and extending in surrounding relation of the card reader slot (12). Nor does Figure 1 show the emitter (108) and detector (102) mounted in supporting connection with such a housing member. Claim 15 is not anticipated.

Claim 16

Appellants' remarks in support of the patentability of claim 1 are incorporated herein by reference. The Action's reference (at page 5, last four lines) to "pulses" is moot as this language does not appear in claim 16 (or any other claim).

For reasons already discussed, Mair does not teach the recited apparatus. For example, Mair does not teach a sensing device that is adapted to sense an unauthorized card reading device positioned adjacent a card reader slot. As previously discussed, Mair does not sense an unauthorized card reading device. At best, Mair tries to prevent use of a card stealing device (false sheet 118), not a false card *reading* device. Thus, Mair does not anticipate claim 16.

Mair also does not teach "prompting" a user to move a card in a card reader slot. Where does Mair teach prompting a user to move a card in a card reader slot? There is no evidence of record whatsoever that Mair prompts a user to move a card in a card reader slot. Mair teaches that "When a user inserts their card 14 in the slot 12, the ATM 10 displays a message on the screen 18, prompting the user to enter their PIN on the keypad 16" (col. 4, lines 37-39). At best, a PIN entry prompt in Mair follows card insertion. Mair's operational sequence is conventional. Mair does not anticipate claim 16.

Mair further does not teach that operation of a radiation emitting device is *dependent* on prompting a user to move a card in a card reader slot. Mair teaches that "signals are emitted by the emitter 108 at timed intervals" (col. 5, lines 32-33). Mair's emitted signals are not dependent on any prompting of a user, especially a prompting to move a card in a card reader slot. Mair's signals appear to be emitted regardless of whether or not a user is even at the ATM. Mair's emitter (108) is not dependent on prompting a user to move a card in a card reader slot. Again, Mair does not anticipate claim 16.

Claim 17

Since Mair does not teach the recited apparatus of claim 16, Mair further cannot teach the additional radiation sensing device of claim 17, which depends on claim 16. Mair does not anticipate claim 17.

Claim 18

Claim 18 depends from claim 17/16. Mair further does not teach a radiation sensing device and a radiation emitting device both positioned adjacent the card reader slot, and where the radiation sensing device can sense radiation emitted by the radiation emitting device. As

previously discussed (e.g., claim 1 remarks), one having ordinary skill in the art would recognize that Mair's emitting device (108) and detector (102) are not "positioned adjacent" the same card reader slot. Mair does not anticipate claim 18.

Claim 19

Appellants' remarks in support of the patentability of claims 1 and 16 are incorporated herein by reference. For reasons already discussed, Mair does not teach the recited apparatus.

Mair further does not teach a radiation emitting device and a radiation sensing device mounted in supporting connection with a "slot member" on a user interface, where the slot member bounds at least one side of a slot. As previously discussed, an exemplary form of the invention includes a radiation emitting device (126) and a radiation sensing device (128) mounted in supporting connection with a slot member (66) (Figures 1 and 14-15). Where in Mair is a radiation emitting device mounted (along with the sensing device 102) in supporting connection with a slot member bounding the slot (12)? Mair's emitting device (108) is not mounted as recited. Mair does not anticipate claim 19.

Claim 24

Claim 24 depends from claim 19. Appellants' remarks in support of the patentability of claim 19 are incorporated herein by reference. Mair further does not teach a radiation emitting device and a radiation sensing device mounted on opposite sides of the same slot and (claim 19) mounted in supporting connection with a slot member that bounds at least one side of the slot. Also note Appellants' claim 14 remarks. Mair does not anticipate claim 24.

Claim 26

Appellants' remarks in support of the patentability of claims 1, 16, 19, and 23 are incorporated herein by reference. For reasons already discussed, Mair does not teach the recited method.

As previously discussed (e.g., claims 1 and 19 remarks), Mair does not teach *both* an emitting device and a radiation sensor device located adjacent to the same card reader slot, especially where the radiation sensor device is located adjacent the emitting device. One having ordinary skill in the art would recognize that Mair's emitting device (108) and detector (102) are not "located adjacent" each other *and* the same card reader slot. Where does Mair even teach that the emitting device (108) and the detector (102) are located adjacent each other? Conversely, Mair specifically shows in Figure 3 that the emitting device (108) is remotely located from both the detector (102) and the slot (12). Mair does not anticipate claim 26.

For reasons previously discussed, Mair also does not teach sensing an unauthorized card reader device attached to the user interface. As previously discussed, at best, Mair tries to prevent use of a card stealing device (false sheet 118), not a false card *reading* device. Mair does not teach sensing an unauthorized card reader device. Again, Mair does not anticipate claim 26.

Claim 29

Claim 29 depends from claim 26. For reasons already discussed (e.g., claim 24), Mair also does not teach a radiation emitting device and a radiation sensing device arranged on opposite sides of the same slot. Mair does not anticipate claim 29.

Claim 32

Appellants' remarks in support of the patentability of claims 1, 16, 19, and 26 are incorporated herein by reference. For reasons already discussed, Mair does not teach the recited method.

Mair does not teach using fuzzy logic. The Office's assertion of fuzzy logic in Mair is not based on any evidence in the record. Thus, Mair cannot anticipate claim 32.

Nor does Mair teach using fuzzy logic in comparing a "sensing" (with a sensing device) to a "stored value" in determining whether an unauthorized card reader device is attached to a user interface. It follows that Mair cannot provide an output responsive to a result of the determining. Again, Mair does not anticipate claim 32.

Although fuzzy logic may be known in other fields of endeavor (e.g., a Microsoft Computer Dictionary), where does Mair discuss or even mention using fuzzy logic, as alleged? Mair doesn't. The Office's assertion of fuzzy logic in Mair is not based on any evidence in the record.

Nor does Mair have any need of fuzzy logic. Conversely, Mair's alarm prevention is based on using a fixed "predetermined time interval" (col. 5, lines 49-50). In Mair, an alarm output is produced based on no signal being detected. Thus, the alarm cannot be produced based on comparing a sensed signal via fuzzy logic. Mair does not anticipate claim 32.

Furthermore, where does Mair execute fuzzy logic in determining whether an unauthorized card reader device is attached to a user interface? For reasons already discussed, Mair doesn't teach sensing an unauthorized card reader device attached to a user interface. At

best, Mair tries to prevent use of a card stealing device (false sheet 118), which is not a false card reading device. Again, Mair does not anticipate claim 32.

The Office's comments on Action page 9 regarding claim 13 and fuzzy logic are without merit. First, the Office relies on unknown "certain circumstances", not a prior art teaching of record. Secondly, as previously discussed, Mair's alarm output is based on no detection of any signal. That is, Mair's alarm is based on a certainty (i.e., whether a signal is detected or whether it isn't detected). Mair's alarm is based on a go/no go basis. The office has not established that Mair's alarm output is based on executing fuzzy logic. One having ordinary skill in the art having a conventional understanding of fuzzy logic (e.g., Microsoft Computer Dictionary) would recognize that Mair's alarm output is not a "form of fuzzy logic", as alleged by the Office.

The 35 U.S.C. § 103 (a) Rejections

The Applicable Legal Standards

Before a claim may be rejected on the basis of obviousness pursuant to 35 U.S.C. § 103, the Patent Office bears the burden of establishing that all the recited features of the claim are known in the prior art. This is known as *prima facie* obviousness. To establish *prima facie* obviousness, it must be shown that all the elements and relationships recited in the claim are known in the prior art. If the Office does not produce a *prima facie* case, then the Appellants are under no obligation to submit evidence of nonobviousness. MPEP § 2142.

The teaching, suggestion, or motivation to combine the features in prior art references must be clearly and particularly identified in such prior art to support a rejection on the basis of obviousness. It is not sufficient to offer a broad range of sources and make conclusory statements. *In re Dembiczak*, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999).

Even if all of the features recited in the claim are known in the prior art, it is still not proper to reject a claim on the basis of obviousness unless there is a specific teaching, suggestion, or motivation in the prior art to produce the claimed combination. *Panduit Corp. v. Denison Mfg. Co.*, 810 F.2d 1561, 1568, 1 USPQ2d 1593 (Fed. Cir. 1987). *In re Newell*, 891 F.2d 899, 901, 902, 13 USPQ2d 1248, 1250 (Fed. Cir. 1989).

Evidence of record must teach or suggest the recited features. Assertions not based on evidence in the record lack substantial evidence support. *In re Zurko*, 258 F.3d 1379, 59 USPQ2d 1693 (Fed. Cir. 2001). Patentability determination must be based on evidence of record. *In re Lee*, 277 F.3d 1338, 61 USPQ2d 1430 (Fed. Cir. 2002).

It is respectfully submitted that the Action requiring appeal does not meet these burdens.

The Claims Are Not Obvious Over Mair

Claims 3-13, 20-23, 25, 27-28, 30-31, and 33-37 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Mair.

Claim 3

Claim 3 depends from claim 2/1. Mair further does not teach or suggest a radiation emitting device that emits visible light. Even the Action (on page 7) admits that in Mair "Lacking is a specific use of a signal in the visible range".

The 35 U.S.C. § 103(a) rejection of claim 3 is based on Mair alone. However, Mair (as admitted by the Office) is devoid of any teaching or suggestion for combining features thereof so as to produce Appellants' recited invention. Appellants respectfully submit that in light of the admitted failure of the solely applied reference to teach or suggest all of the recited features and relationships, combined with the lack of any other supporting evidence of record, the rejection is not legally valid. The rejection is improperly based on mere assertion and not concrete evidence of record. That is, the record lacks evidential support for the rejection. *In re Zurko*, supra. *In re Lee*, supra. The Office has not established a *prima facie* case of obviousness.

Furthermore, Mair specifically teaches against using visible light. Mair prefers that the emitter and the detector utilize infra-red radiation because it is invisible to humans, and the presence of such a monitoring system would *not* be apparent to users (col. 2, lines 29-33). Also, Mair's ATM fascia portion (114) is transparent to infra-red radiation but *not* transparent to visible light (col. 5, lines 26-29). That is, Mair's system could not operate with visible light. Thus, Mair specifically teaches emitting radiation that is not visible to humans. In light of Mair's explicit

teaching, the Office's presented rational for modification is not reasonable. The Office has not established a *prima facie* case of obviousness.

Claim 4

Claim 4 depends from claim 2/1. Mair further does not teach or suggest emitting radiation during at least one of a transaction step when a user card is to be inserted in the slot and a further transaction step when a user card is to be taken from the slot. Even the Action (on page 7) admits that in Mair does not teach or suggest the recited features.

The 35 U.S.C. § 103(a) rejection of claim 4 is based on Mair alone. Appellants respectfully submit that in light of the admitted failure of Mair to teach or suggest all of the recited features and relationships, the rejection is not legally valid. The rejection is improperly based on mere assertion and not concrete evidence of record. *In re Zurko*, supra. *In re Lee*, supra. The Office has not established a *prima facie* case of obviousness.

The Office has not presented any evidence of record that Mair teaches or suggests that radiation would be emitted during (1) when a user card is to be inserted in the slot, or (2) when a user card is to be taken from the slot. Nor has the Office shown that Mair would need to emit radiation during these short time periods. Furthermore, Mair explicitly teaches that the alarm is prevented during normal usage of the ATM (col. 5, lines 4-10 and 46-53). One skilled in the art would recognize that Mair is not concerned with radiation detection when a card needs to be inserted or removed. Nor is there any teaching or suggestion of Mair having a controller that links radiation emitting to when a card is to be inserted or taken from the slot. The Office has not factually established a *prima facie* case of obviousness.

Claim 5

Claim 5 depends from claim 4/2/1. Mair further does not teach or suggest the ability to cause a value corresponding to a property of radiation *sensed* by the radiation sensing device to be stored in a data store. Where does Mair store in a data store a value corresponding to a sensed property of radiation? Even if Mair taught (which he doesn't) a stored "baseline" as alleged in the Action (at page 7), the baseline would be fixed. Mair does not teach or suggest that the alleged baseline would be that of a *sensed* radiation property value. The Office has not established a *prima facie* case of obviousness.

Claim 6

Claim 6 depends from claim 5/4/2/1. For reasons already discussed, Mair further does not teach or suggest the ability to compare a stored sensed radiation property value with a current sensed radiation property value. Nor does the Action state where Mair allegedly teaches or suggests the recited subject matter. The Office has not established a *prima facie* case of obviousness.

Claim 7

Claim 7 depends from claim 6/5/4/2/1. Mair further does not teach or suggest the ability to compare a stored radiation property value with a current radiation property value (e.g., claim 6) to determine a difference (e.g., claim 7). Where does Mair determine a difference?

Nor does Mair teach or suggest that responsive to determining the difference, causing a *status message* to be sent by the machine to a remote computer. The relied upon section of Mair at col. 5, lines 40-45 refers to activation of an "alarm circuit", not to the ATM sending a message to a remote computer. The Office has not established a *prima facie* case of obviousness.

Claim 8

Claim 8 depends from claim 6/5/4/2/1. Mair further does not teach or suggest the ability to compare a stored radiation property value with a current radiation property value (e.g., claim 6) to determine a difference (e.g., claim 8). Where does Mair determine a difference?

Nor does Mair teach or suggest that responsive to determining the difference, causing an output message to be output (locally) through an output device on the user interface. Where does Mair provide an output at the ATM? Conversely, Mair teaches that the alarm is for an ATM operator who is located away from the ATM. Note that Mair distinguishes a remote ATM operator from a local ATM user (col. 1, lines 56-59; col. 2, lines 9-11; col. 3, lines 21-24 and 34-37; and col. 5, lines 1-3 and 42-45). The Office appears to try to improperly interchange Mair's ATM operator and ATM user.

The allegation at Action page 8 that Mair's "ATM is deactivated if an object is detected, this would certainly somehow, be reflected on the user interface" is without factual support. The Action's relied upon "somehow" language smacks of pure speculation. Regardless, how could a message "be output through at least one output device on the user interface" if Mair's ATM was not even active? The Office has not established a *prima facie* case of obviousness.

Claim 9

Claim 9 depends from claim 8/6/5/4/2/1. Mair further does not teach or suggest having a message output (locally) at the ATM that advises of a possible object near the slot. Mair's alarm is for notifying the ATM operator, not the ATM user. Mair specifically teaches that the alarm is remotely located from the ATM for the benefit of the ATM operator (col. 1, lines 56-59; col. 2, lines 9-11; col. 3, lines 21-24 and 34-37; and col. 5, lines 1-3 and 42-45). The Office appears to

try to improperly interchange Mair's ATM operator and ATM user. As previously discussed in the claim 8 remarks, Mair distinguishes a remote ATM operator from a local ATM user. The Office has not established a *prima facie* case of obviousness.

Claim 10

Claim 10 depends from claim 6/5/4/2/1. Mair further does not teach or suggest the ability to change the stored sensed radiation property value responsive to a current sensed radiation property value. Even if Mair taught (which he doesn't) a stored "baseline" as alleged in the Action (at page 8 for claim 5), the baseline would be fixed. Mair does not teach or suggest that the alleged baseline would be changed, especially in response to a current *sensed* radiation property value. The Office has not established a *prima facie* case of obviousness.

Claim 11

Claim 11 depends from claim 3/2/1. Mair further does not teach or suggest at least one radiation emitting device that can illuminate a card reader slot. Where does Mair teach or suggest that the emitter (108) *both* emits radiation and illuminates a card reader slot? As previously discussed (claim 3 remarks), Mair specifically teaches against emitting radiation that is visible to humans. Where does Mair teach or suggest the ability to both guide a user to the card reader slot (via the illumination) and sense an unauthorized card reading device adjacent to the card reader slot? The Office has not established a *prima facie* case of obviousness.

Claim 12

Claim 12 depends from claim 6/5/4/2/1. Mair further does not teach or suggest the ability to compare the stored sensed radiation property value with a current sensed radiation property

value at a time when a transaction is not being conducted by a user at the apparatus. The Office has not established a *prima facie* case of obviousness.

Claim 13

Claim 13 depends from claim 6/5/4/2/1. Mair further does not teach or suggest executing fuzzy logic in comparing a current sensed radiation property value with a stored sensed radiation property value. Although fuzzy logic may be known in other fields of endeavor (e.g., a Microsoft Computer Dictionary), where does Mair discuss or even mention using fuzzy logic, as alleged? Mair doesn't. Additionally note Appellants' comments concerning Mair and fuzzy logic with regard to claims 23 and 32. The Office has not established a *prima facie* case of obviousness.

Claim 20

Claim 20 depends from claim 16. Mair further does not teach or suggest the ability to store in the data store a value responsive to a signal from the sensing device; compare the stored value to a current value (which corresponds to a signal currently produced by the sensing device); and produce the output responsive to a result of the comparison (and sensed unauthorized card reading device). The Office has not established a *prima facie* case of obviousness.

Claim 21

Claim 21 depends from claim 16. Mair further does not teach or suggest producing a status message as a result of comparing a stored value to a current value (which corresponds to a signal currently produced by the sensing device). The Office has not established a *prima facie* case of obviousness.

Claim 22

Claim 22 depends from claim 20/16. Mair further does not teach or suggest the ability to cause a stored value to be changed responsive to a current value. Even if Mair taught (which he doesn't) a stored "baseline" as alleged in the Action (at page 8 for claim 5), the baseline would be fixed. Mair does not teach or suggest that the alleged baseline would be changed, especially in response to a currently produced value. The Office has not established a *prima facie* case of obviousness.

Claim 23

Appellants' remarks in support of the patentability of claims 1 and 32 are incorporated herein by reference. For reasons already discussed, Mair does not teach or suggest the recited apparatus.

For reasons previously discussed, Mair does not teach or suggest the ability to sense an unauthorized card reading device. As previously discussed, at best, Mair tries to prevent use of a card stealing device (false sheet 118), which is not a false card *reading* device. That is, Mair does not teach or suggest sensing an unauthorized card reading device.

Although fuzzy logic may be known in other fields of endeavor (e.g., a Microsoft Computer Dictionary), where does Mair discuss or even mention using fuzzy logic, as alleged? Mair doesn't. Mair at the relied upon col. 5, lines 45-55, does not teach or suggest execution of fuzzy logic.

The Office's assertion of fuzzy logic in Mair is not based on any evidence in the record. However, the law requires that the evidence of record must teach or suggest the recited features in order to establish a valid rejection. *In re Zurko*, supra. *In re Lee*, supra.

Nor does Mair have any need of fuzzy logic. Conversely, Mair's alarm prevention is based on using a fixed "predetermined time interval" (col. 5, lines 49-50). In Mair, an alarm output is produced based on no signal being detected. Thus, the alarm cannot be produced based on comparing a sensed signal via fuzzy logic. The Office has not established a *prima facie* case of obviousness.

Furthermore, where does Mair execute fuzzy logic in *comparing* a stored value to a current value (corresponding to a sensed signal), especially where an output is produced responsive to a *result of the comparison*. In Mair an output (i.e., alarm) is produced based on no signal being detected. The alarm is not produced in response to a comparison of signals. That is, Mair does not "produce at least one output responsive to a result of the comparison". The Office has not established a *prima facie* case of obviousness.

The Office's comments on Action page 9 regarding claim 13 and fuzzy logic are without merit. First, the Office relies on unknown "certain circumstances", not a prior art teaching of record. Secondly, as previously discussed, Mair's alarm output is based on no detection of any signal. That is, Mair's alarm is based on a certainty (i.e., whether a signal is detected or whether it isn't detected). Mair's alarm is based on a go/no go basis. The office has not established that Mair's alarm output is based on executing fuzzy logic. One having ordinary skill in the art having a conventional understanding of fuzzy logic (e.g., Microsoft Computer Dictionary) would recognize that Mair's alarm output is not a "form of fuzzy logic", as alleged by the Office.

Claim 25

Claim 25 depends from claim 24/19. Appellants' remarks in support of the patentability of claims 3, 11, 14 are incorporated herein by reference. Mair further does not teach or suggest a

slot member that extends in generally surrounding relation of a card slot, and a radiation emitting device that is operative to visibly illuminate an area surrounding the card slot. Where does Mair teach or suggest the recited "slot member"? Where does Mair teach or suggest that the emitter (108) *both* emits radiation and illuminates a card slot? As previously discussed (e.g., claim 3 remarks), Mair specifically teaches against emitting radiation that is visible to humans. That is, Mair specifically teaches against the recited invention. The Office has not established a *prima facie* case of obviousness.

Claim 27

Claim 27 depends from claim 26. Since Mair does not teach or suggest the recited method of claim 26, Mair further cannot teach or suggest sending a status message from the machine responsive to sensing an unauthorized card reader device as recited in claim 27. The Office has not established a *prima facie* case of obviousness.

Claim 28

Claim 28 depends from claim 26. Appellants' remarks in support of the patentability of claims 8 and 9 are incorporated herein by reference. Mair further does not teach or suggest providing a notice indicating the presence of a possible unauthorized reader device to a *user of the machine* through at least one output device. Where does Mair output a notice to an ATM user of a possible unauthorized reader device? As previously discussed, Mair's alarm is remotely located from the ATM. Mair's alarm is for notifying the ATM operator, not the ATM user. The Office appears to try to improperly interchange Mair's ATM operator and ATM user. As previously discussed (e.g., claim 8 remarks), Mair distinguishes a remote ATM operator from a

local ATM user (col. 1, lines 56-59; col. 2, lines 9-11; col. 3, lines 21-24 and 34-37; and col. 5, lines 1-3 and 42-45). The Office has not established a *prima facie* case of obviousness.

Claim 30

Claim 30 depends from claim 29/26. For reasons already discussed (e.g., remarks to claims 6, 20, and 23), Mair further does not teach or suggest comparing a property of radiation sensed from a sensor device to a stored value. The Office has not established a *prima facie* case of obviousness.

Claim 31

Claim 31 depends from claim 30/29/26. For reasons already discussed (e.g., remarks to claims 10 and 22), Mair also does not teach or suggest changing a stored value responsive to radiation sensed. The Office has not established a *prima facie* case of obviousness.

Claim 33

Claim 33 depends from claim 26. For reasons already discussed (e.g., remarks to claims 3 and 25), Mair also does not teach or suggest operating a radiation emitting device to emit visible light. Where does Mair teach or suggest that the emitter (108) emits visible light? As previously discussed, Mair specifically teaches against emitting radiation that is visible to humans.

Nor is there any evidence of record that Mair teaches or suggests operating the emitter (108) when a card is to be removed from the slot. The rejection is based on pure speculation and not concrete evidence of record. *In re Zurko*, supra. *In re Lee*, supra. The Office has not factually established a *prima facie* case of obviousness.

Claim 34

Claim 34 depends from claim 33/26. For reasons already discussed (e.g., remarks to claims 11 and 25), Mair also does not teach or suggest that a radiation emitting device illuminates a card reader slot. The Office has not established a *prima facie* case of obviousness.

Claim 35

Appellants' remarks in support of the patentability of claims 1, 16, 19, 23, 26, and 32 are incorporated herein by reference. For reasons already discussed, Mair does not teach or suggest the recited method.

Mair does not teach or suggest that any sensing actually occurs in a transaction step in which a card is to be moved in a card reader slot. Where is this step taught or suggested in Mair? The rejection is not based on concrete evidence of record. The Office has not established a *prima facie* case of obviousness.

For reasons already discussed, Mair also doesn't teach or suggest determining an unauthorized card reader device is attached to the user interface (step b). At best, Mair tries to prevent use of a card stealing device (118), which is not an unauthorized *card reading* device. The Office has not established a *prima facie* case of obviousness.

Even if it were somehow possible (which it isn't) for Mair to determine that an unauthorized card reader device is attached to the user interface, Mair still wouldn't teach or suggest recited step (b). Step (b) is "responsive to step (a)". That is, Mair still would not teach or suggest "determining an unauthorized card reader device is attached to the user interface *responsive to*" "operating at least one sensing device adjacent to a card reader slot . . . in a

transaction step in which a card is to be moved in the card reader slot". The Office has not established a *prima facie* case of obviousness.

Mair further does not teach or suggest (step c) that *in response to* determining an unauthorized card reader (step b), capturing a card (that has been subject to being read by the determined unauthorized card reader). Where does Mair teach or suggest the recited card capturing procedure?

The Action (on page 11) asserts that "If the card is in the ATM when it is deactivated it would likely remain in the ATM". The Office's assertion is unreasonable. For example, the Office has not presented any evidence of record that in Mair a user card would be in the ATM at the time of the alleged determining of an unauthorized card reader (or during the alleged ATM deactivation). Conversely, Mair's system can "accommodate normal usage of the ATM" such "that use of the card reader slot 12 by a user . . . will not result in issue of spurious alarm signals" (col. 5, lines 46-53).

If Mair's ATM is immediately deactivated upon indication of fraud (as alleged by the Office), then it is designed such that deactivation would occur *before* a user card could even be inserted in the ATM. That is, a card wouldn't even be in Mair's ATM when it is deactivated, let alone be captured by the ATM. Mair's system would not permit a user card to have "been subject to being read" (step c) by an unauthorized card reader. If Mair's user card was never subject to being read, then why would it need to be captured by the ATM? The rejection is based on impermissible hindsight reconstruction of Appellants' claimed invention. *In re Fritch*, supra. The Office has not established a *prima facie* case of obviousness.

Furthermore, even if it were somehow possible (for the sake of argument) for Mair to have a card "in the ATM when it is deactivated" (which Mair actually teaches against), Mair still wouldn't teach or suggest recited step (c). There would still be no teaching or suggestion that the card would be captured through operation of the ATM. What specific teaching or suggestion in Mair prevents or limits the card from being returned by the ATM to the user prior to (or during) the deactivation? At best, a card in Mair is captured by the false card slot, not through any operation of the ATM. The rejection is based on pure speculation and not concrete evidence of record. *In re Zurko*, supra. *In re Lee*, supra. The Office has not factually established a *prima facie* case of obviousness.

Additionally, the Action's noted assertion of "If the card is in the ATM when it is deactivated it would *likely* remain in the ATM" (on page 11) along with the rejection, is based on ifs, likelihoods, and pure speculation. Again the rejection is not based on concrete evidence of record. Conversely, Appellants have established that a card won't even be in Mair's ATM when it is deactivated. Thus, a card can't be captured by Mair's ATM. Again, the Office has not factually established a *prima facie* conclusion of obviousness.

Claim 36

Appellants' remarks in support of the patentability of claim 35 are incorporated herein by reference. For reasons already discussed (e.g., claim 35 remarks), Mair does not teach or suggest recited steps (a) or (b).

Mair also does not teach or suggest recited step (c). Mair does not teach or suggest that *responsive to determining an unauthorized card reader, cancelling an account* (associated with a

card that has been subject to being read by the unauthorized card reader). Where does Mair teach or suggest cancelling an account? Mair doesn't.

The Action's allegation that an ATM *user* in Mair would cancel their account "responsive to" determining (step b) an unauthorized card reader is without basis. Where does Mair teach or suggest notifying the ATM user (or making the user aware) of an unauthorized card reader? As previously discussed many times, Mair's alarm is for notifying a remote ATM operator, not the ATM user. Mair's alarm is remotely located from the ATM user. The Office appears to try to improperly interchange Mair's ATM operator and ATM user. However, Mair distinguishes a remote ATM operator from a local ATM user (col. 1, lines 56-59; col. 2, lines 9-11; col. 3, lines 21-24 and 34-37; and col. 5, lines 1-3 and 42-45).

Additionally, for reasons previously discussed (e.g., claim 35 remarks), Appellants have established that a user card in Mair would not have "been subject to being read" (step c) by an unauthorized card reader. Mair's ATM would be deactivated before a card could even be read. If the card was never subject to being read, then why would an account need to be canceled? The Office has not factually established a *prima facie* conclusion of obviousness.

The statement in the Action (on page 11) that "This examiner has taken that kind of action in the past" is noted. The reliance by the Examiner on a previous action in an unknown and unrelated application (which does not appear to be of record) should have no bearing with regard to the current application.

Claim 37

Appellants' remarks in support of the patentability of claims 35 and 36 are incorporated herein by reference. For reasons already discussed (e.g., claims 35 and 36 remarks), Mair does not teach or suggest recited steps (a) or (b).

Mair also does not teach or suggest recited step (c). Mair does not teach or suggest monitoring activity on an account, especially *responsive to* determining an unauthorized card reader. For reasons previously discussed (e.g., claim 35 remarks), Appellants have established that a user card in Mair would not have "been subject to being read" (step c) by an unauthorized card reader. Mair's ATM would be deactivated before a card could even be read. If the card was never subject to being read, then why would activity on the card's account need to be monitored? The Office has not factually established a *prima facie* conclusion of obviousness.

The statement in the Action (on page 11) that "This examiner has taken that kind of action in the past" is noted. Again, the reliance by the Examiner on a previous action in an unknown and unrelated application (which does not appear to be of record) should have no bearing with regard to the current application.

CONCLUSION

Each of Appellants' pending claims specifically recites features, relationships, and/or steps that are neither disclosed nor suggested in the applied prior art. Furthermore, the applied prior art is devoid of any teaching, suggestion, or motivation for combining features of the applied prior art so as to produce the recited invention. For these reasons it is respectfully submitted that all the pending claims are allowable.

Respectfully submitted,

Tom J

Ralph E. Jockey
WALKER & JOCKE
231 South Broadway
Medina, Ohio 44256
(330) 721-0000



(viii)

CLAIMS APPENDIX

1. An automated banking machine apparatus comprising:
 - a housing;
 - a user interface in supporting connection with the housing, the user interface including at least one input device and at least one output device, wherein the at least one input device includes a card reader having an associated card reader slot adapted to accept cards input by users of the apparatus;
 - at least one radiation emitting device positioned adjacent the slot;
 - at least one radiation sensing device adjacent the slot such that positioning an unauthorized card reading device adjacent the slot causes a change in at least one property of radiation from the at least one radiation emitting device that is sensed by the at least one radiation sensing device;
 - at least one controller in the housing, wherein the at least one controller is in operative connection with the at least one radiation sensing device and is operative to generate at least one signal responsive to the change, whereby installation of an unauthorized card reading device adjacent the slot is indicated.

2. The apparatus according to claim 1 and further comprising a currency dispensing device in supporting connection with the housing.
3. The apparatus according to claim 2 wherein the at least one radiation emitting device is operative to emit visible light.
4. The apparatus according to claim 2 wherein the controller is operative to cause the apparatus to carry out a currency dispensing transaction, and wherein the controller is operative to cause the at least one radiation emitting device to initiate emitting radiation during at least one of a transaction step when a user card is to be inserted in the slot and a further transaction step when a user card is to be taken from the slot.
5. The apparatus according to claim 4 and further comprising at least one data store, wherein the controller is operative to cause at least one stored value corresponding to the at least one property of radiation sensed by the at least one radiation sensing device to be stored in the data store.
6. The apparatus according to claim 5 wherein the controller is operative to compare the at least one stored value with at least one current value corresponding to the at least one property of radiation currently sensed by the at least one radiation sensing device.

7. The apparatus according to claim 6 wherein the controller is operative responsive to determining a difference when comparing the at least one stored value to the at least one current value to cause a status message to be sent by the machine to a remote computer.
8. The apparatus according to claim 6 wherein the controller is operative responsive to determining a difference when comparing the at least one stored value to the at least one current value to cause an output message to be output through at least one output device on the user interface.
9. The apparatus according to claim 8 wherein the output message advises of a possible object near the slot.
10. The apparatus according to claim 6 wherein the controller is operative to change the at least one stored value responsive to the at least one current value.
11. The apparatus according to claim 3 wherein the at least one radiation emitting device is adapted to surroundingly illuminate the card reader slot.
12. The apparatus according to claim 6 wherein the controller is operative to compare the at least one stored value with the at least one current value at a time when a transaction is not being conducted by a user at the apparatus.

13. The apparatus according to claim 6 wherein the controller is operative to execute fuzzy logic in comparing the at least one current value with the at least one stored value.
14. The apparatus according to claim 1 and further comprising a housing member bounding at least one side of the card reader slot, and wherein the at least one radiation emitting device and the at least one radiation sensing device are mounted in supporting connection with the housing member.
15. The apparatus according to claim 14 wherein the housing member extends in surrounding relation of the card reader slot.
16. An automated banking machine apparatus comprising:
 - a housing;
 - a user interface in supporting connection with the housing,
wherein the user interface includes at least one input device and at least one output device,

wherein the at least one input device includes a card reader having an associated card reader slot adapted to accept cards input by users of the machine;

at least one radiation emitting device;

at least one sensing device,

wherein the at least one sensing device is adapted to sense an unauthorized card reading device positioned adjacent the card reader slot;

at least one controller in the housing and in operative connection with the at least one radiation emitting device and the at least one sensing device,

wherein the controller is operative to cause prompting of a user to move a card in the slot,

wherein the at least one controller is operative to selectively cause operation of the at least one radiation emitting device,

wherein the operation is dependent on the prompting

wherein the at least one controller is operative to cause at least one output responsive to a sensing of an unauthorized card reading device.

17. The apparatus according to claim 16 wherein the at least one sensing device comprises at least one radiation sensing device.
18. The apparatus according to claim 17 wherein the at least one sensing device and the at least one radiation emitting device are both positioned adjacent the card reader slot, wherein the at least one radiation sensing device is adapted to sense radiation emitted by the at least one radiation emitting device.
19. An automated banking machine apparatus comprising:
 - a user interface,
 - a slot member on the user interface and bounding at least one side of a slot,
 - at least one sensor device positioned to detect an unauthorized object placed adjacent the user interface,

wherein the at least one sensor device includes at least one radiation emitting device and at least one radiation sensing device mounted in supporting connection with the slot member,

at least one controller,

wherein the at least one controller is operative to selectively control the at least one sensor device.

20. The apparatus according to claim 16 wherein the at least one controller is in operative connection with at least one data store,

and wherein the at least one controller is operative to

cause to be stored in the at least one data store at least one stored value responsive to at least one signal from the at least one sensing device,

compare the at least one stored value to at least one current value corresponding to at least one signal currently produced by the at least one sensing device, and

produce the at least one output responsive to a result of the comparison.

21. The apparatus according to claim 16 wherein the at least one output comprises a status message.
22. The apparatus according to claim 20 wherein the at least one controller is further operative to cause the at least one stored value to be changed responsive to the at least one current value.
23. An automated banking machine apparatus comprising:
 - a housing,
 - a user interface in supporting connection with the housing, the user interface including at least one input device and at least one output device, wherein the at least one input device includes a card reader having an associated card reader slot adapted to accept cards input by users of the machine,
 - at least one sensing device positioned adjacent the card reader slot, wherein the at least one sensing device is adapted to sense an unauthorized card reading device positioned adjacent the card reader slot,
 - at least one controller in the housing and in operative connection with the at least one sensing device, wherein the at least one controller is operative to execute

fuzzy logic in comparing at least one stored value and at least one current value corresponding to at least one signal currently produced by the at least one sensing device, and wherein the at least one controller is operative to produce at least one output responsive to a result of the comparison.

24. The apparatus according to claim 19 wherein at least one radiation emitting device and at least one radiation sensing device are mounted on opposite sides of the slot.
25. The apparatus according to claim 24 wherein the slot comprises a card slot, wherein the slot member extends in generally surrounding relation of the card slot, and the at least one radiation emitting device is operative to visibly illuminate an area surrounding the card slot.
26. A method comprising:
 - (a) sensing with at least one sensing device adjacent to a card reader slot of a user interface of an automated banking machine, an unauthorized card reader device attached to the user interface,

wherein the sensing includes emitting radiation with at least one emitting device located adjacent the slot;

wherein the sensing includes sensing radiation from the at least one emitting device with at least one radiation sensor device located adjacent the slot and the at least one emitting device;

wherein the sensing device is selectively controlled by at least one controller of the machine;

(b) responsive to sensing the unauthorized card reader device, providing at least one output from the machine.

27. The method according to claim 26 wherein step (b) comprises sending a status message from the machine.
28. The apparatus according to claim 26 wherein step (b) comprises providing a notice indicating presence of a possible unauthorized reader device to a user of the machine through at least one output device.
29. The method according to claim 26 wherein at least one emitting device and at least one radiation sensor device are arranged on opposite sides of the slot, and wherein step (a) comprises:

sensing radiation emitted from an opposite side of the slot.

30. The apparatus according to claim 29 wherein step (a) further comprises:

comparing at least one property of radiation sensed from the at least one sensor device to at least one stored value.

31. The method according to claim 30 and further comprising:

(c) operating the at least one emitting device when no unauthorized card reader device is sensed;

(d) sensing radiation emitted in step (c) with at least one radiation sensor device;

(e) changing the at least one stored value responsive to radiation sensed in step (d).

32. A method comprising:

(a) operating at least one sensing device adjacent to a card reader slot of a user interface of an automated banking machine;

- (b) executing fuzzy logic in comparing at least one property of a sensing with the at least one sensing device to at least one stored value in determining whether an unauthorized card reader device is attached to the user interface; and
 - (c) responsive to determining an unauthorized card reader device is attached, providing at least one output from the machine.
33. The method according to claim 26 wherein the at least one emitting device emits visible light during operation, and further comprising:
- (c) operating the at least one emitting device when the machine conducts a transaction step in which a card is to be removed from the slot.
34. The method according to claim 33 and prior to step (c) further comprising:
- dispensing currency from the machine, and wherein in step (c) the at least one emitting device illuminates the slot in generally surrounding relation.
35. A method comprising:

- (a) operating at least one sensing device adjacent to a card reader slot of a user interface of an automated banking machine in a transaction step in which a card is to be moved in the card reader slot;
- (b) determining an unauthorized card reader device is attached to the user interface responsive to step (a);
- (c) responsive to step (b), capturing a card that has been subject to being read by the unauthorized reading device through operation of the machine.

36. A method comprising:

- (a) operating at least one sensing device adjacent to a card reader slot of a user interface of an automated banking machine in a transaction step in which a card is to be moved in the card reader slot;
- (b) determining an unauthorized card reader device is attached to the user interface responsive to step (a);
- (c) responsive to step (b), cancelling an account associated with a card that has been subject to being read by the unauthorized reading device.

37. A method comprising:

- (a) operating at least one sensing device adjacent to a card reader slot of a user interface of an automated banking machine in a transaction step in which a card is to be moved in the card reader slot;
- (b) determining an unauthorized card reader device is attached to the user interface responsive to step (a);
- (c) responsive to step (b), monitoring activity on an account associated with a card that has been subject to being read by the unauthorized reading device.

38. (withdrawn) A method comprising:

- (a) sensing with at least one sensing device adjacent to a card reader slot of a user interface of an automated banking machine, an unauthorized object adjacent to the card reader slot, wherein the at least one sensing device is selectively controlled by at least one controller of the machine;
- (b) responsive to the sensing in step (a), providing at least one output from the machine, wherein the at least one output includes requesting at least one

user input to the machine corresponding to an appearance of the user interface adjacent to the card reader slot;

- (c) receiving user input with the machine responsive to step (b);
- (d) operating the at least one controller to determine whether the unauthorized object sensed in step (a) is an unauthorized card reader device attached to the user interface responsive to the user input received in step (c); and
- (e) responsive to determining an unauthorized card reader device in step (d), providing at least one other output from the machine.

(ix)

EVIDENCE APPENDIX

(None)

(x)

RELATED PROCEEDINGS APPENDIX

(None)